# Creating a Software Assurance Body of Knowledge

Samuel T. Redwine Jr.
*James Madison University*

*The Software Assurance Workforce Education and Training Working Group, composed of government, industry, and academic members, is currently taking a first step toward achieving adequate U.S. education and training on software assurance. It is defining the additional body of knowledge needed to acquire, develop, and sustain secure software beyond that normally required to produce and assure software where safety and security are not concerns.*

In 2003, the Department of Defense (DoD) launched a software assurance initiative. In 2004, the Department of Homeland Security (DHS) joined in collaboration with DoD and other agencies and established its own Software Assurance Program[1], and DoD and DHS began to jointly sponsor semiannual software assurance forums.

While the term *software assurance* potentially encompasses assuring any property or functionality of software, the initiative encompasses safety and security and integrates practices from a number of disciplines (see Figure 1). Initially, the effort has concentrated on achieving and assuring security properties and functionality. This includes not only activities during development, but also the acquisition and sustainment processes.

This is driven by a growing demand for low-defect, secure software for crucial roles in defense and commerce often performed by commercial off-the-shelf products. However, current commonplace software specification, design, implementation, and testing practices provide users with software containing numerous defects and security vulnerabilities. Hence, the initiatives' Workforce Education and Training Working Group is currently addressing achievement of adequate U.S. education and training on software security, including training within government and industry, and curriculum needs within universities, colleges, and trade schools.

## Defining Software Assurance Common Body of Knowledge

After deliberation, the working group decided to first create a description of the additional needed knowledge – beyond that required for *normal* software – to acquire, develop, and sustain secure software, including assurance of its security properties and functionality. The working group first identified the activities or aspects of activities relevant to secure software – beyond normal activities – and then asked, "What knowledge is needed to perform these activities?" Three difficult sub-questions exist:

1. What are the normal activities and their normal aspects?
2. What are the additional activities or aspects of activities that are relevant?
3. What knowledge is needed to perform these added activities?

Initially, the subgroup addressing software development has taken the Software Engineering Body of Knowledge Guide [1] as a working description of what is the normal knowledge.

The efforts to answer the second question benefit from a number of prior efforts, including the following:

- National Cyber Security Partnership Task Force report on "Processes to Produce Secure Software" [2].
- Safety and Security Extensions for Integrated Capability Maturity Models [3].
- National Institute of Standards and Technology Information System Security Project.

The working group also benefits from the expertise of its members and the work of other working groups and reviewers.

Some key knowledge not widely known even though associated with normal activities may be included. The intent is to ensure adequate coverage of requisite knowledge areas to enable professionals playing a number of roles in software engineering, systems engineering, and program management to identify knowledge and acquire competencies associated with software assurance. Because of this wide coverage and applicability, the intended product is officially called the "Software Assurance Common Body of Knowledge."

After several rounds of internal and external review, the initial report should include an introduction followed by four parts describing and identifying references for the additional knowledge required:

1. Common concepts and principles required across acquiring, developing, and sustaining secure software.
2. Development.
3. Post-Release Sustainment.
4. Acquisition and Supply.

The Software Assurance Common Body of Knowledge, initially released Oct. 3 at the DHS-DoD co-sponsored Software Assurance Forum, will be updated after public review and published in December 2005.◆

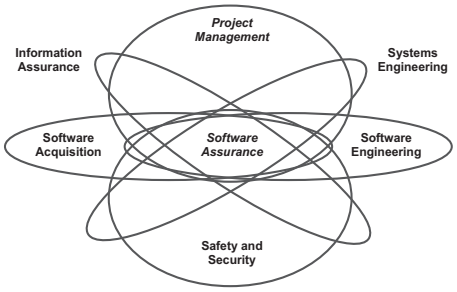


Figure 1: *Disciplines Contributing to Software Assurance*

## References

1. Institute of Electrical and Electronics Engineers. Guide to the Software Engineering Body of Knowledge. Eds. P. Bourque and R. Dupuis. 2004 ed. Los Alamitos, CA: IEEE, 16 Feb. 2004.
2. National Cyber Security Partnership. Processes for Producing Secure Software: Towards Secure Software. Vols. I and II. Eds. S.T. Redwine Jr. and N. Davis. Washington: National Cyber Security Partnership, 2004.
3. Ibrahim, Linda, et al. Safety and Security Extensions for Integrated Capability Maturity Models. Washington: Federal Aviation Administration, Sept. 2004 <www.faa.gov/ipg>.

## Note

1. See <http://BuildSecurityIn.us-cert.gov> for information about the DHS Software Assurance Program and related products.

## Author Contact

**Samuel T. Redwine Jr.**
**James Madison University**
**Computer Science MSC 4103**
**Harrisonburg, VA 22807**
**Phone: (540) 568-6305**
**E-mail: redwinst@jmu.edu**